

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

THE REYNOLDS & REYNOLDS  
COMPANY

Plaintiff,

vs.

SUPERIOR INTEGRATED SOLUTIONS,  
INC.

Defendant.

Case No. 1:12-cv-00848

District Judge Thomas M. Rose

**THE REYNOLDS & REYNOLDS COMPANY'S RESPONSE TO  
SUPERIOR INTEGRATED SOLUTIONS, INC.'S RENEWED EMERGENCY MOTION  
FOR PRELIMINARY INJUNCTION (DKT. #28)**

**INTRODUCTION**

SIS's Motion (Dkt. #28) is based on two false premises: (1) that Reynolds accessed SIS's "internal" website, obtained protected and proprietary information, and then used that information to disable SIS's integration software; and (2) that SIS has a legally protected right to hostilely integrate third-party applications with Reynolds' proprietary automobile dealer management system ("DMS") known as ERA. These premises are unfounded, and SIS's Motion fails.

Reynolds filed this case upon learning that SIS had copied Reynolds' copyrighted "ERAccess" software program file in order to hostilely integrate certain uncertified third-party applications with Reynolds' DMS. SIS never disputed that the program file had been copied, but instead professed ignorance as to *who* copied it and placed it in SIS's program directory on dealership computers. Reynolds then ran a Google search and easily traced the copied software

to SIS: it was available for download on a publicly accessible website sponsored and maintained by SIS.

Backed into a corner, SIS sent Reynolds two vague “cease and desist” letters baldly suggesting that, in catching SIS red-handed with Reynolds’ copyrighted software, Reynolds had somehow wrongfully accessed **its own software** (and other unspecified information) from SIS’s website. SIS then filed this “emergency” motion for injunctive relief, which paints the misleading picture that Reynolds ignored SIS’s letters. *See* Dkt. #28, at PageID 188-89, Exs. B-1 & B-2 (attaching SIS’s letters of Feb. 13 and 15, 2013). But Reynolds had responded promptly and in great detail on February 13 and 18, 2013 (*see* Exs. B and C hereto)—SIS simply failed to mention these responses in its Motion. SIS’s intentional omission speaks volumes.

SIS’s second key premise—that SIS somehow has the right to integrate third-party applications with Reynolds’ DMS without Reynolds blocking or disabling the unauthorized integration software—is equally frivolous. First, SIS’s argument is barred by the preclusive effect of this Court’s order dismissing the prior lawsuit between SIS and Reynolds, *Superior Integration Solutions, Inc. v. The Reynolds and Reynolds Company*, Case No. 3:09-cv-314 (S.D. Ohio) (Rose, J.) (the “2009 Action”). Second, SIS’s position has no basis in law or fact—which is likely why SIS’s 2009 Action was abandoned. For all of these reasons, SIS’s Motion should be denied.

## **BACKGROUND**

### **I. SIS Seeks the Same Relief Here that it Failed to Obtain in the 2009 Action**

In 2009, SIS filed a Complaint and Motion for Temporary Restraining Order against Reynolds, complaining that Reynolds was terminating SIS’s contractual right under the Reynolds Interface Agreement (“RIA”) to provide certified integration services between third-party

application providers and Reynolds' DMS. *See* Complaint (Dkt. #1) in 2009 Action; Motion for TRO (Dkt. #5) in 2009 Action. SIS explained that an "integrator" like itself could integrate with Reynolds' DMS in one of two ways: either (1) pursuant to an agreement with Reynolds (e.g., the RIA) or (2) without Reynolds' permission or assistance (a/k/a "hostile" integration). *See* Motion for Preliminary Injunction (Dkt. #20-1) in 2009 Action at PageID 227-28; Affidavit of Phillip Battista (Dkt. #20-2) in 2009 Action at ¶¶ 9-11 (PageID 247-48).

Though SIS had been integrating with Reynolds' DMS since 2006 under the RIA, that agreement was set to expire on September 21, 2009. SIS sought a judicially created "wind-down" period that would have extended the RIA beyond its stated expiration date. *See* Dkt. #1 in 2009 Action at ¶¶ 1, 15-19, 44-58 (PageID 61, 64, 69-70). SIS acknowledged that, upon termination of the RIA, it would have to revert to the cat-and-mouse process of hostile integration, which entails the following:

1. SIS installs code on dealership computers to integrate third-party applications with Reynolds' proprietary DMS without care or regard to the impact it may have on the Reynolds DMS from a security or performance perspective.
2. In the process of constantly updating its software to improve the functionality of its DMS, correct defects that arise from time to time, and address a host of issues including performance and security issues caused by hostile integration, Reynolds issues general software updates and security patches that can (and frequently do) "disable" SIS's hostile integration of third-party applications.
3. When these updated software modifications and security enhancements cause SIS's integration software to fail, SIS endeavors to modify its software in such a way as to navigate around Reynolds' modifications, and the process starts again.

Ex. A (Decl. of Kelly Hall) at ¶¶ 5, 8-9, 12, 16-17; *see also* Injunction Hearing Transcript (Dkt. #25) in 2009 Action at PageID 456-62.

Prior to the RIA, SIS relied for years on hostile integration methods to access Reynolds' DMS and, therefore, recognized that the end of the RIA would ensure a renewed cat-and-mouse

game. *See* Dkt. #25 in 2009 Action at PageID 456-62. SIS filed the 2009 Action in an attempt to buy more time to modify its integration programs to evade security patches. *See id.* at PageID 494 (“[I]n the absence of injunctive relief . . . Reynolds will start enacting or erecting wholesale, across-the-board security patches that will interfere or block the current integration that SIS is providing.”); *id.* at PageID 494-95 (requesting injunctive relief “because SIS has not yet been able . . . to come up with a system to convert all [21 third party application provider customers] to an alternate integration.”).

Although SIS ultimately focused its strategy in the 2009 Action on seeking a contractual “wind-down” period, SIS could have asserted (and to an extent, did assert) the very same claims that it now asserts in the present case challenging Reynolds’ right to block hostile integration with its DMS. *See* Dkt. #1 in 2009 Action at ¶¶ 63-79 (PageID 71-74) (alleging counts of Tortious Interference with Business Relationships, Tortious Interference with Contract, and Unfair or Deceptive Trade Practices). While SIS did not literally allege violations of the Sherman Antitrust Act or the Computer Fraud and Abuse Act (“CFAA”) in the 2009 Action, SIS at least implied these theories—and certainly understood Reynolds’ security policies and practices with respect to hostile third-party integration. *See* Dkt. #25 in 2009 Action at PageID 494; *see also* Dkt. #1 in 2009 action at ¶¶ 28-30 (PageID 66) (describing Reynolds’ threat to “remove, disable, or otherwise block SIS’s integration software” and SIS’ response that “such action . . . would constitute a tortious interference with SIS’s . . . business and contractual relationships”); *id.* at ¶ 24 (PageID 65) (describing Reynolds’ “anti-competitive pricing proposals for the new RIA”); SIS’s Response to Reynolds’ Notice of Compliance (Dkt. #40) in 2009 action at PageID 662 n.2 (“SIS notes that Reynolds’ knowing transmission of a computer

program . . . that impairs the integrity of a separate computer program . . . without authorization is also prohibited by the [CFAA].”).

Regardless of the specific reason why SIS chose to focus on the “wind-down” strategy in the 2009 Action—i.e., whether SIS (i) perceived that the potential benefits of extending the RIA were better than embarking on a new chapter of the cat-and-mouse game, (ii) recognized that an antitrust or similar theory lacked merit, or (iii) for some other reason entirely—SIS chose its path in the 2009 Action and failed. This Court rejected SIS’s claim that it was entitled under the RIA to more time to prepare for the inevitable cat-and-mouse battle and denied such injunctive relief. *See* Orders (Dkt. ##26 & 28) in 2009 Action.

As a result, the parties agreed to settle and dismiss the case, and on June 21, 2010 this dismissed “any and all claims and counterclaims asserted or raised in this action, *as well as all claims arising out of or in connection with the matters described in this action*” with prejudice. Dkt. #61 in 2009 Action.

## **II. Reynolds’ Policy of Blocking Hostile Integrators is Not Controversial**

Reynolds’ practice of issuing security patches that disable hostile third-party application integration is essential to maintaining the security of dealership data, including the private information of their customers, and to ensure the efficient operation of the DMS the customers have licensed. *See* Ex. A at ¶¶ 5, 9, 12. (The copyright violations at issue in this lawsuit were actually discovered as a result of DMS malfunctions caused by SIS’s hostile integration. Ex. A at ¶¶ 18-19). In any event, the security process is fully authorized by Reynolds’ customers.

Pursuant to their license of Reynolds’ ERA and associated software (e.g., “ERAccess”), Reynolds’ customers agree not to permit uncertified third parties to integrate with the ERA DMS, and they consent to the installation by Reynolds of security patches and updates. *See* Ex.

A at ¶¶ 10-15; *see also, e.g.*, Reynolds Customer Guide (Ex. A-2) at 19 (“Unless we [Reynolds] provide otherwise, you [the customer] may not install Other Matter on the Equipment or connect Other Matter to Licensed Matter, either directly or remotely, without our prior written consent”); *id.* at 21 (“You shall not . . . attempt to create or discover, by any means, . . . integration to other programs. . . .”).

Reynolds periodically issues updates to its customers to improve ERA functionality and to protect data security and operational integrity of the overall DMS. When Reynolds issues such updates, the installation process is automatic: updates are “pushed” from the ERA server to the relevant files and folders on individual dealership PCs, and outdated versions are overwritten as part of an update. Ex. A at ¶ 12. Reynolds’ customers agree to every aspect of this process, including that:

- Reynolds has authorized access to their systems at all times to perform maintenance, software updates, and other services, Ex. A-2 at 8-9;
- the customers must use the most recent version of ERA software, *id.* at 24;
- Reynolds can remotely load software enhancements (or require that the customers’ load them), *id.* at 15-16; and
- such enhancements may overlay the functionality of third-party software, *id.* at 16.

Reynolds’ practices do not, as SIS claims, have the effect of eliminating competition in the broad DMS application market, or even the purported “Reynolds-brand DMS application market.” To the contrary, Reynolds routinely certifies third-party applications used by Reynolds’ customers to operate with Reynolds’ DMS. Certification guarantees that third-party applications are integrated with Reynolds’ DMS and protected from security patches. To date, 144 third-party application providers with 172 applications have been certified by Reynolds (or “pre-certified,” with final documentation pending). *See* Ex. A at ¶ 7. At least 26 of those

providers were certified since the time the 2009 Action was filed, including some of the most significant competitors in the industry—e.g., AutoTrader.com, J.D. Power and Associates, and DealerTrack’s eMenu. *Id.*

In light of these facts, it is not surprising that SIS made no serious argument in the 2009 Action that Reynolds could not issue security patches or disable SIS integration once the RIA was terminated, or that SIS had some fundamental right independent of the RIA to integrate with Reynolds’ DMS. As this Court recognized, Reynolds is allowed to block or disable SIS’s integration software.<sup>1</sup> *See* Reynolds’ Motion for Clarification (Dkt. #27) in 2009 Action; Clarification Order (Dkt. #28) in 2009 Action.

### **III. The Present Case: SIS Copied Reynolds’ Software to Aid Hostile Integration**

Moving forward to the present action, Reynolds and SIS engaged in the above-described cat-and-mouse game since the 2009 Action. In 2012, however, SIS tried a new approach. Confronted with a more secure, updated version Reynolds’ ERAccess software, SIS copied the old version of ERAccess’s primary executable file, renamed it “sysdiagx.exe,” and installed that version in the SIS “directory” on dealership computers. Reynolds first uncovered SIS’s actions in August 2012, when a dealer complained of “auto log-off” problems, a feature that had changed between the version of ERAccess improperly copied by SIS to the next version of ERAccess. Ex. A at ¶¶ 18-19. At the dealer’s request (and with the dealer’s authorization), Reynolds personnel remotely logged into the dealership’s PC and identified the source of the

---

<sup>1</sup> In the 2009 Action, Reynolds represented through its counsel that it would not literally remove SIS’s software from a dealership’s computers without that dealership’s permission. SIS later argued that Reynolds violated its representation by removing what are known as “VOC entries” from an SIS file. Reynolds responded, *inter alia*, that the VOC entries were not SIS’s code. Ultimately, the Court sided with SIS and ordered Reynolds to place the VOC entries back into the SIS files, which Reynolds promptly did. Dkt. # 37 in the 2009 Action. The Court refused, however, to grant SIS additional relief or to modify its order **recognizing Reynolds’ right to disable SIS’s software by other means**. Dkt. ## 40 & 42 in the 2009 Action.

problem as an outdated version of ERAccess. *Id.* at ¶ 18. Subsequently, Reynolds was able to identify the “sysdiagx.exe” file as an exact copy of Reynolds’ outdated version of ERAccess. *Id.* at ¶¶ 18-19.

In November 2012, Reynolds filed this lawsuit and implemented enhancements designed to verify that dealers are running the current version of ERAccess. Ex. A at ¶ 20. Since November, Reynolds has not implemented any additional new patches or security enhancements intended to combat SIS’s hostile integration (though it had and continues to have every right to do so). *Id.*

#### **IV. SIS’s Contention that Reynolds Acted Improperly is a Farce**

On December 26, 2012, almost two months after this lawsuit was filed, SIS sent Reynolds a letter acknowledging the existence of sysdiagx.exe (nicknamed “the Patch” by SIS) but disclaimed any responsibility or knowledge regarding its creation:

Contrary to R&R’s accusations, SIS did not create the Patch. In fact, SIS was unaware of the very existence of the Patch until R&R brought the issue to SIS’s attention. . . . Therefore, . . . the Patch could only have been placed there surreptitiously and without the authorization of SIS—a clear cause of concern for SIS.

Ex. D at 1-2.

It was easy to prove that SIS was not telling the truth. Representatives of Reynolds literally ran a Google search and located the sysdiagx.exe file on a publicly accessible website sponsored and maintained by SIS (“uset.datadms.com”). Ex. A at ¶ 21. In other words, Reynolds’ copyrighted executable file was available on SIS’s website for downloading to dealership computers (or anywhere else with an internet connection). Reynolds amended its Complaint to include this information. *See* Dkt. # 22.



Upon receipt of Reynolds' Amended Complaint, SIS cut off public access to this web page. Ex. A at ¶ 21. No longer able to disclaim responsibility for "the Patch," SIS took a different tack: on February 13, 2013, SIS accused Reynolds of essentially hacking into SIS's internal computer system and "using information wrongfully obtained from SIS to willfully and intentionally block access to dealers' DMS at stores throughout the country." 2/13/12 Letter from M. Ornstein (Dkt. # 28, Ex. B). SIS then threatened to seek injunctive relief and seek "the harshest sanctions available" unless Reynolds took certain unspecified actions in response to unspecified allegations. *Id.* Reynolds promptly responded that same day, pointing out that: (i) only a few weeks earlier, SIS had claimed that SIS had nothing to do with "sysdiagx.exe," (ii) shortly after receiving the Amended Complaint, SIS disabled public access to the "downloads" page on which "sysdiagx.exe" had been posted; and (iii) most importantly, Reynolds truly could not discern what SIS wanted it to cease and desist from. 2/13/12 Letter from G. Harvey (Ex. B hereto).

On Friday, February 15, 2013, apparently unaware that Reynolds had found the "sysdiagx.exe" file on SIS's publicly accessible internet site, SIS sent a letter accusing Reynolds of improperly accessing "an internal website used by SIS support staff." 2/15/2013 Letter from M. Ornstein (Dkt. # 28, Ex. B-2). SIS further accused Reynolds of somehow using information obtained from that website to interfere with SIS's integration software, and SIS made demand on Reynolds that it "cease and desist these activities." *Id.*

On Monday, February 18, 2013, Reynolds sent SIS another detailed response explaining that the "sysdiagx.exe" file was located using a Google search on a publicly accessible website maintained and sponsored by SIS. 2/18/2013 Letter from G. Harvey (Ex. C hereto). Once again,

Reynolds asked SIS to explain clearly and directly what conduct it believed Reynolds should “cease and desist” from. *Id.* SIS made no reference in its Motion to either of Reynolds’ letters.

On February 19, 2013, Reynolds’ counsel spoke with SIS’s counsel. During that call, the case was discussed in detail, but SIS’s counsel made no mention of any action from which Reynolds needed to cease and desist. Nor did SIS provide any clarity regarding its allegations at any other time prior to filing its February 25, 2013 “Emergency” Motion for Preliminary Injunction.

## **ARGUMENT AND AUTHORITIES**

### **I. Due to SIS’s Conduct, this Court Should Reject SIS’s Request for Injunctive Relief**

SIS copied Reynolds’ copyrighted software for its own profit. Now that SIS has been caught red-handed, it has boldly asked this Court to enter an injunction protecting its patently unlawful conduct. Indeed, SIS has asked this Court to enjoin Reynolds from “interfering with the interfacing between SIS’s integration software and Reynolds’ [DMS],” Dkt. #28 at PageID 181, in full knowledge that at least one way that such interfacing has occurred is via SIS’s own brazen violation of the Copyright Act. Simply put, SIS’s Motion mocks this Court’s charge to enforce federal laws.

Further, SIS has attempted to shield its unlawful actions from scrutiny, first by misrepresenting facts to Reynolds and then by attempting to cover its tracks by disabling public access to the web page on which “sysdiagx.exe” had been posted. And throughout this time period, SIS has sent Reynolds threatening letters and neglected to inform this Court about Reynolds’ relevant responses, all in an apparent effort to create the contrived appearance that Reynolds has been ignoring SIS. SIS’s actions are textbook examples of unclean hands and should bar its request for equitable relief. *See, e.g., Sherfel v. Gassman*, 748 F. Supp. 2d 776,

789 (S.D. Ohio 2010) (“The doctrine of unclean hands may be invoked by a court to deny injunctive relief where the party applying for such relief is guilty of conduct involving fraud, deceit, unconscionability, or bad faith related to the matter at issue to the detriment of the other party” provided that “the alleged misconduct on the part of the plaintiff relate directly to the transaction about which the plaintiff has made a complaint.”); CHARLES. A. WRIGHT ET AL., FED. PRAC. AND PROCEDURE 2d, § 2946, at 106 (1995) (“As a matter of public policy, equitable relief will not be granted to an individual who has acted in bad faith with respect to the transaction that has been brought before the court.”); *cf. Original Great Am. Chocolate Chip Cookie Co. v. River Valley Cookies, Ltd.*, 970 F.2d 273 (7th Cir. 1992) (finding that preliminary injunction requiring restoration of franchise agreement should have been denied because the franchisees infringed franchisor’s trademarks). SIS’s Motion should be denied outright.

## **II. SIS’s Counterclaims are Barred by Res Judicata**

Under applicable *res judicata* principles, a subsequent action is barred when the following four elements are met: “(1) a final judgment by a court of competent jurisdiction; (2) a subsequent action between the same parties or their privies; (3) an issue in the subsequent action which was litigated or which could have been litigated in the prior action; and (4) an identity of the causes of action.” *Hekfrich v. Metal Container Corp.*, 11 F. App’x 574, 576 (6th Cir. 2001) (applying Ohio law). “Identity” does not require that the elements or the evidence required to prove the claims at issue actually be identical—rather, the requirement is met if the causes of action arise from “the same transaction, or series of transactions,” *id.*, that is, they arise from a “common nucleus of operative facts.” *Grava v. Parkman Township*, 653 N.E.2d 226, 229 (Ohio 1995).

Each element is met here. The parties are identical (Element 2), and this Court’s order dismissing with prejudice “any and all claims and counterclaims asserted or raised in [the 2009 Action], *as well as all claims arising out of or in connection with the matters described in this action*” is a final judgment (Element 1). *See* Dkt. # 61 in 2009 Action; *ABS Indus., Inc. ex rel. ABS Litig. Trust v. Fifth Third bank*, 333 F. App’x 994, 998 n.3 (6th Cir. 2009). Further, SIS’s antitrust, CFAA, and tortious interference claims all could have been litigated in the prior action (Element 3). SIS was well aware of Reynolds’ ability and intention to issue security patches once the RIA expired and SIS was no longer certified, but SIS simply made the strategic decision to seek injunctive relief under its meritless “wind-down” theory rather than press the claims it asserts now. *See Grava*, 653 N.E.2d at 229 (noting that claim preclusion “applies to extinguish a claim by the plaintiff . . . [e]ven though the plaintiff is prepared in the second action . . . to seek remedies or forms of relief not demanded in the first action.”). With respect to Element 4, the nucleus of facts has not changed since the end of the 2009 Action: SIS has (and had) no integration agreement with Reynolds and thus needs (and needed) to navigate around Reynolds’ security patches. Since there is no meaningful difference between the factual and evidentiary bases for SIS’s 2009 and current claims, claim preclusion bars the current action. *See id.* (“The doctrine of *res judicata* requires a plaintiff to present every ground for relief in the first action, or be forever barred from asserting it.” (internal quotations omitted)).

### **III. Even if SIS’s Claims are Not Formally Barred, Equitable Principles Weigh Strongly Against Injunctive Relief**

SIS’s Motion also violates the equitable maxim that a party “cannot rely on its own deliberate actions to create the harm it hopes to avoid as a basis for seeking injunctive relief.” *Damon’s Restaurants, Inc. v. Eileen K Inc.*, 461 F. Supp. 2d 607, 626–27 (S.D. Ohio 2006). SIS deliberately sought to dismiss the 2009 Action with prejudice, fully aware that the cat-and-mouse

game would proceed and that its integration services and third-party application provider clients would be subject to Reynolds' security patches. SIS's request in this case for injunctive relief is an attempt to escape the obvious consequences of its prior decision. Accordingly, relief should be denied. *See Chicago Title Ins. Corp. v. Magnuson*, No. 2:03-CV-368, 2005 WL 2373430, at \*28 (S.D. Ohio Sept. 26, 2005) (finding that balance of harms weighs against party that incurred self-inflicted hardships), *reversed in part on other grounds by* 487 F.3d 985 (6th Cir. 2007).

Moreover, the timing of the Motion casts serious doubts on SIS's allegations of "irreparable harm." Nearly *three years* have passed since SIS and Reynolds resumed the non-RIA cat-and-mouse game, and for three years Reynolds has issued patches and enhancements that could potentially interfere with SIS's hostile integration. Yet, SIS never sought injunctive relief against Reynolds' conduct until it was caught violating Reynolds' copyrights. Moreover, even assuming for the sake of argument that SIS's suggestions of lost revenue and corporate goodwill are accurate, those are problems entirely of SIS's own making: SIS chose to hinge its business fortunes on its ability to succeed at hostile integration in a post-RIA world. This Court correctly rejected this very same irreparable-harm theory from SIS in the 2009 Action, noting that "a party may not rely upon its own deliberate actions to create harm as a basis for seeking injunctive relief." Dkt. #26 in 2009 Action at PageID 448. Now, three years removed from the RIA, SIS's "irreparable harm" argument is, if anything, far weaker.

#### **IV. SIS Has No Right to Integrate and No "Strong Likelihood of Success on the Merits"**

Even if the Court does not determine that SIS's claims are barred outright, SIS cannot establish a likelihood of success on the merits of any of them. In addition to the legal deficiencies set forth below (and in Reynolds' concurrently filed Motion to Dismiss Amended

Counterclaim (Dkt. # 29)), SIS's claims fundamentally fail because SIS has no *right* to hostilely integrate third-party applications with Reynolds' DMS in the first place.

**A. SIS's Antitrust Claims Cannot Succeed on the Merits**

SIS asserts two largely identical antitrust violations focused on the alleged single-brand "aftermarket for third-party applications designed to integrate with Reynolds-DMS system at auto dealerships." Dkt. #28 at PageID 191. According to SIS, Reynolds' practice of implementing security patches and blocking hostile third party applications from its DMS gives rise to a Section 1 "tying" claim and a Section 2 "monopolization" claim. There are several fundamental problems with SIS's antitrust theories. First, SIS fails to establish a relevant market for antitrust purposes. Second, SIS fails to establish that Reynolds had or exercised requisite market power or injured competition in any relevant market. Third, even if one were to assume the existence of the implausible and conclusory "aftermarket for third-party applications designed for Reynolds DMS" suggested by SIS, SIS is not a competitor or consumer in that alleged market and, thus, lacks antitrust standing.

**1. SIS Fails to Establish a Relevant Market**

To state a claim under Section 1 or 2 of the Sherman Act, the plaintiff must define the relevant market in which competition has been injured. With respect to a Section 1 tying claim, the plaintiff must establish two markets: the "tying product" and the "tied product." *See Arnold v. Petland, Inc.*, No. 2:07-CV-013707, 2009 WL 816327, \*4 (S.D. Ohio Mar. 26, 2009) ("For example, a supermarket that will sell flour to consumers only if they will also buy sugar is engaged in tying. Flour is referred to as the tying product, sugar as the tied product.").

To establish a relevant market in the Sixth Circuit, one must apply the "reasonable interchangeability" standard, which requires evaluating: geography, product use (i.e. "whether

the substitute products or services can perform the same function”), quality, description, and consumer response / cross elasticity—that is, “consumer sensitivity to price levels at which they elect substitutes for the defendant’s product or service.” *Worldwide Basketball and Sport Tours, Inc. v. Nat’l Collegiate Athletic Ass’n*, 388 F.3d 955, 961 (6th Cir. 2004). SIS steers well clear of this analysis, presumably because it recognizes that any focus on the numerous non-Reynolds DMS choices available to customers dooms SIS’s antitrust theories. As set forth in more detail in section IV(A)(2) *infra*, consumers have multiple primary DMS providers to choose from, and routinely switch DMS providers for reasons that include dissatisfaction with the third-party applications available for that DMS, or for no reason at all. Ex. A at ¶ 3.

In an attempt to manufacture an artificial, “Reynolds DMS-only” universe, SIS relies on a narrow exception to the standard of “reasonable interchangeability,” articulated in *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451 (1992). “That exception allows for a narrower market definition—a single brand market that does not include available substitutes—where a plaintiff has become ‘locked-in’ by making an initial purchase of or investment in a defendant’s product.” *Shamrock Mktng., Inc. v. Bridgestone Bandag, LLC*, 775 F. Supp. 2d 972, 982 (W.D. Ky. 2011).

But *Kodak* does not apply to a situation where, as here, the supposed “lock in” is simply an informed contractual choice by the consumer. The Sixth Circuit has explained:

We likewise agree that the change in policy in *Kodak* was the crucial factor in the Court’s decision. By changing its policy after its customers were “locked in,” Kodak took advantage of the fact that its customers lacked the information to anticipate this change. Therefore, it was Kodak’s own actions that increased its customers’ information costs. In our view, this was the evil condemned by the Court and the reason for the Court’s extensive discussion of information costs. . . . [W]e thus hold that an antitrust plaintiff cannot succeed on a *Kodak*-type theory when the defendant has not changed its policy after locking-in some of its customers, and the defendant has been otherwise forthcoming about its pricing structure and service policies.

*PSI Repair Servs., Inc. v. Honeywell, Inc.*, 104 F.3d 811, 820 (6th Cir. 1997); *see also Laserworks v. Pitney Bowes*, No. C2-96-1307, 1999 WL 33435671, at \*6–8 (S.D. Ohio Dec. 29, 1999) (discussing *PSI Repair Servs.*). Reynolds’ restrictions against uncertified applications connecting to Reynolds’ DMS are readily apparent in Reynolds’ Customer Guide. *See supra* at 5-7. There are no increased customer information costs, and *Kodak* does not apply.

For the same reasons, *In re Apple AT & TM Antitrust Litig.*, 596 F. Supp. 2d 1288 (N.D. Cal. 2008)—a *Kodak* violation case—does not apply. *See Apple Inc. v. Psystar*, 586 F. Supp. 2d 1190, 1202 (N.D. Cal. 2008) (dismissing antitrust claim alleging single-brand aftermarket for Apple operating systems because customers knew Apple computers could only be used with Apple operating systems and distinguishing *AT & TM* because in that decision the allegation was that Apple customers purchased the iPhone without knowing of an undisclosed exclusive voice-and-data service contract with AT & TM); *In re ATM Antitrust Litig.*, 738 F. Supp. 2d 984, 996–97 (N.D. Cal. 2009) (discussing *Psystar* and *AT & TM* and dismissing antitrust claims on the same basis as *Psystar*).

Moreover, of course, *Kodak* involved the complete elimination of competition in the tied market, which as explained below, is a critical fact that is totally absent here.

## **2. SIS Fails to Establish Market Power or Injury to Competition**

Even if SIS successfully identified a relevant market (which it has not done), SIS fails to establish that Reynolds possessed appreciable market power in any such market. SIS thus fails to establish antitrust injury. “To prove antitrust injury, the key inquiry is whether competition—not necessarily a competitor—suffered as a result of the challenged business practice.” *Wee Care Child Center, Inc. v. Lumpkin*, 680 F.3d 841, 847 (6th Cir. 2012). SIS does not and cannot prove this element.



First, the primary DMS market—the only conceivable “tying product” market—is subject to robust competition. Dealerships routinely switch DMS providers: in 2012 alone, 467 dealership customers left Reynolds for another DMS provider, and 141 new customers switched to Reynolds. Ex. A at ¶ 3. Moreover, contrary to SIS’s vague allegation that Reynolds is the “largest provider” of DMS in the country, occupying a “large percentage” of the market, *see* Dkt. #28 at PageID 185, Reynolds’ U.S. market share is less than 35%, well down from where it was at the time of the 2009 Action. *See id.*

Second, assuming for the sake of argument that the “tied product” market is the purported “aftermarket for third-party applications designed for Reynolds DMS” (as SIS contends), there is no indication that any injury to competition has occurred there either. As SIS acknowledges, any third-party application provider that wishes can choose to become certified by Reynolds and sell applications that connect to Reynolds’ DMS. Dkt. #25 at ¶ 12 (PageID 166). Well over one hundred certified third-party application providers (not owned in any manner by Reynolds) sell applications that work with the Reynolds DMS. *See* Ex. A at ¶ 7; *see also* Dkt. #25 in 2009 Action at PageID 459 (SIS admits that “[m]any companies, dozens if not hundreds, [go the non-certified route]. . . . SIS did it for years before September of 2006.”). In sum, Reynolds has no “market power” and has not caused anything resembling an “antitrust injury.”

### **3. SIS Fails to Establish Antitrust Standing**

Finally, even a plaintiff that can establish an antitrust injury must also establish “antitrust standing”—i.e., that the plaintiff “is a proper party to bring a private antitrust action.” *Associated Gen. Contractors of Cal., Inc. v. Cal. State Council of Carpenters*, 459 U.S. 519, 537 n.31 (1983) (“*AGC*”). “[S]tanding in an antitrust case is more onerous than the conventional Article III inquiry.” *Static Control Components, Inc. v. Lexmark Intern., Inc.*, 697 F.3d 387, 402

(6th Cir. 2012). Even giving SIS the benefit of the doubt on every other shortcoming of its antitrust claims, SIS fails to establish antitrust standing.

Barring a narrow exception not applicable to this case, “only claimants who are *competitors or consumers* within the injured market have standing to sue.” *Lexmark*, 697 F.3d at 404 (emphasis added).<sup>2</sup> Further, “[w]here there are more-direct victims of the anticompetitive conduct, those victims have the standing to sue, rather than those affected indirectly.” *Id.* at 405. Here, SIS is not—and does not claim to be—a competitor or consumer in any “third-party application market”—whether limited to Reynolds-compatible applications, or otherwise. *See* Dkt. #28, Ex. A, Phillip Battista Aff., ¶ 6 (describing SIS only as a provider of “integration software” whose “direct customers” are the third-party application providers). If anyone would have standing under the antitrust theory posited by SIS (putting aside the other fatal flaws of that theory), it would be third-party application developers themselves. SIS does not have standing to pursue the antitrust claims advanced in its Motion.

#### **B. SIS’s CFAA Claim Cannot Succeed on the Merits**

Not only is SIS’s CFAA claim three years too late—clearly, this claim could have been asserted in the 2009 Action—it is also legally flawed. SIS appears to assert claims under § 1030(a)(5)(A) of the CFAA—the so-called “transmission” liability provision. But any alleged transmissions by Reynolds are wholly authorized by its DMS customers. Pursuant to the Reynolds customer agreements, Reynolds’ customers: (1) agree not to integrate third-party applications with Reynolds’ DMS without Reynolds’ permission; and (2) authorize Reynolds to

---

<sup>2</sup> The exception to this rule applies where a defendant “manipulated or utilized [the plaintiff] as a fulcrum, conduit or market force to injure competitors or participants in the relevant product and geographical markets.” *Lexmark*, 697 F.3d at 404. Here, SIS has not made any such allegations (plausible or otherwise).

(a) access their computers for software updates and to diagnose software malfunctions, (b) transmit updates, and (c) transmit security patches. *See* Ex. A at ¶¶ 10-15.

Courts recognize that such “voluntary” transmission acceptances sever CFAA “transmission” liability. *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1066, 1068 (N.D. Cal. 2012) (listing cases and finding no CFAA violation because “Apple had authority to access the iDevice . . . as a result of the voluntary installation of the software (either as an update or native installation).”); *see also In re Apple & ATTM Antitrust Litig.*, No. C 07-05152 JW, 2010 WL 3521965, at \*7 (N.D. Cal. July 8, 2010), *vacated in part on other grounds*, 826 F. Supp. 2d 1168 (N.D. Cal. 2011) (“Voluntary installation runs counter to the notion that the alleged act was a trespass and to CFAA's requirement that the alleged act was ‘without authorization’ as well as the CPC's requirement that the act was ‘without permission.’”). SIS’s CFAA claim will not succeed on the merits.

### **C. SIS’s Tortious Interference Claim Cannot Succeed on the Merits**

Finally, SIS seeks injunctive relief for Reynolds’ alleged interference with SIS’s integration contracts. However, the very contracts on which SIS seeks relief necessarily contemplate breaches of Reynolds’ own customer agreements’ integration prohibitions. Ohio law allows Reynolds to enforce its contracts, even if that enforcement “interferes” with SIS’s contracts. Thus, SIS’s position is fatally flawed.

Under Ohio law, “one is privileged to purposely cause another not to perform a contract with a third person where he in good faith is asserting a legally protected interest of his own, which he believes will be impaired or destroyed by the performance of a contract.” *Wright v. MetroHealth Med. Ctr.*, 58 F.3d 1130, 1139 (6th Cir. 1995); *see also* RESTATEMENT OF THE LAW

(TORTS) SECOND § 773 (1979). Reynolds' customer agreements allow it to take the actions of which SIS now complains. Thus, SIS's tortious interference claim also goes nowhere.

**V. The Remaining “Balancing Factors” Weigh Against Granting an Injunction**

Putting aside the unlikelihood of SIS succeeding on the merits, the remaining factors that courts typically balance when deciding a motion to injunction—namely, (i) irreparable harm to the movant; (ii) substantial harm to the respondent; and (iii) public interest—also weigh heavily against SIS's Motion. *See* Dkt. #26 in 2009 Action (citing *Tumblebus Inc. v. Cranmer*, 399 F.3d 754, 759 (6th Cir. 2005)). With respect to these factors, the Court's analysis in the 2009 Action still stands—in both instances, SIS's motions boil down to an attempt to obtain judicial protection of a purported right that SIS never contracted for. *See generally id.*; *supra* Section III (regarding irreparable harm).

**CONCLUSION**

For all of these reasons, Reynolds respectfully requests that SIS's Renewed Motion for a Preliminary Injunction (Dkt. #28) be denied.

Respectfully submitted,

**BIESER, GREER & LANDIS LLP**

By: /s/ James H. Greer  
David C. Greer, Trial Attorney (0009090)  
James H. Greer, Trial Attorney (0046555)  
400 PNC Center  
6 North Main Street  
Dayton, Ohio 45402-1908  
Telephone: 937-223-3277  
Telecopier: 937-223-6339  
E-MAIL [dcg@bgllaw.com](mailto:dcg@bgllaw.com); [jhg@bgllaw.com](mailto:jhg@bgllaw.com)

**GIBBS & BRUNS LLP**

Grant Harvey, SBN 09177700, admitted *pro hac vice*  
Aundrea K. Gulley, SBN 24034468, admitted *pro hac vice*  
Brian T. Ross, SBN 24037395, admitted *pro hac vice*  
Ben Bireley, SBN 24076086, admitted *pro hac vice*  
1100 Louisiana, Suite 5300  
Houston, TX 77002  
Telephone: 713-650-8805  
Telecopier: 713-750-0903

**CERTIFICATE OF SERVICE**

The undersigned certifies that, pursuant to Local Rule CV 5.2(b), the foregoing document was served electronically through the Court's CM/ECF system on all counsel who are registered users of the system as provided in Fed. R. Civ. P. 5(b)(2)(E). Any counsel of record not deemed to have registered for such electronic service were served with a true and correct copy of the foregoing by U.S. mail on this 25th day of March, 2013.

/s/ James H. Greer  
James H. Greer